

## Lecture 4

C. Skinner (2)

$$\mathbb{Z}_p = \left\{ (a_n) \in \prod \mathbb{Z}/p^n : a_{n+1} \equiv a_n (p^n)^2 \right\} = \varprojlim \mathbb{Z}/p^n \text{ (projective limit)}$$

$R_p = \{0, 1, 2, \dots, p-1\}$  complete set of representatives of the residue classes mod  $p$

• each integer  $m$  is congruent mod  $p$  to a unique elt of  $R_p$ .

$R_n = \left\{ \sum_{i=0}^{n-1} r_i p^i : r_i \in R_p \right\}$  complete set of representatives of residue classes mod  $p^n$

$$a \in \mathbb{Z}_p \quad a = (r_n) ; r_n \in R_n$$

$$\text{if } r_{n+1} = \sum_{i=0}^n r_i p^i \text{ then } r_n = \sum_{i=0}^{n-1} r_i p^i ; a \mapsto \sum_{i=0}^{\infty} r_i p^i \quad r_i \in R_i$$

$$\mathbb{Z}_p \leftrightarrow \left\{ \sum_{i=0}^{\infty} r_i p^i : r_i \in R_i \right\}$$

$$(a_n) \text{ when } a_n = \sum_{i=0}^{n-1} r_i p^i$$

Obviously multiplication / addition of RNS is the same as that in  $\mathbb{Z}_p$  "base  $p$ ".

$$-1 \leftrightarrow 1 \cdot 2^0 + 1 \cdot 2 + 1 \cdot 2^2 + \dots + 1 \cdot 2^{n-1}$$

$$\left( \frac{1}{2} \frac{1}{2^2} \dots \right)$$

$$(r_0 + r_1 p + \dots)(s_0 + s_1 p + s_2 p^2) = (r_0 s_0 + (r_0 s_1 + r_1 s_0)p + \dots)$$

$p$ -adic valuation

$$\text{ord}_p(\dots) : \mathbb{Q}_p \rightarrow \mathbb{Z} \cup \{-\infty\}$$

$$\forall x \in \mathbb{Q}_p \quad x = p^k a ; a \in \mathbb{Z}_p^* ; k \in \mathbb{Z} \text{ - unique.}$$

$$\text{ord}_p(x) := k \quad \text{ord}_p(0) = +\infty$$

$$\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y) ; x = p^k a ; y = p^l b ; xy = p^{k+l} ab$$

$$\text{ord}_p(x) = 0 \iff x \in \mathbb{Z}_p^* \quad \boxed{x \neq 0}$$

$$\text{ord}_p(\frac{1}{x}) = -\text{ord}_p(x)$$

$$\text{ord}_p = \text{homomorphism} : \mathbb{Q}_p^\times \rightarrow \mathbb{Z}$$

$$\text{ord}_p(x) \geq 0 \iff x \in \mathbb{Z}_p ; -\text{ord}_p(x) \geq n \iff x \in p^n \mathbb{Z}_p$$

$$\text{ord}_p(x+y) \geq \min \{ \text{ord}_p(x), \text{ord}_p(y) \} = \text{if } \text{ord}_p(x) \neq \text{ord}_p(y)$$

$$x = p^k u ; y = p^l v ; k \leq l ; x+y = p^l (v+p^{k-l} u)$$

$$\text{Examples: } \text{ord}_2(\frac{3}{5}) = 0$$

$$\text{ord}_3(\frac{3}{5}) = 1$$

$$\text{ord}_5(\frac{3}{5}) = -1$$

$$\in \mathbb{Z}_p$$

$$\text{ord}_2(\frac{3}{5} + 1) = \text{ord}_2(\frac{8}{5}) = 2$$

$$\text{ord}_3(\frac{3}{5} + 1) = \text{ord}_3(\frac{8}{5}) = 0$$

$$\text{ord}_5(\frac{3}{5} + 1) = \text{ord}_5(\frac{8}{5}) = -1$$

$p$ -adic absolute value:

$$|\cdot|_p : \mathbb{Q}_p \rightarrow \mathbb{R}_{\geq 0}$$

$$|x|_p = p^{-\text{ord}_p(x)} \quad (1 \text{ if } p=0)$$

$$-|x+y|_p \leq p^{-\min \{ \text{ord}_p(x), \text{ord}_p(y) \}}$$

$$|x|_p = p^{-k}$$

$$-|xy|_p = |x|_p \cdot |y|_p$$

$$= |x|_p \cdot |y|_p$$

Lecture 4

Ostrowski's Thm

$f: \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$  s.t.

$$(i) f(x) = 0 \iff x = 0$$

$$(ii) f(xy) = f(x) \cdot f(y)$$

(iii)  $f(x+y) \leq f(x) + f(y)$  then either

$$(a) f(x) = 1 \quad \forall x \neq 0$$

$$(b) f(x) = |x|_p, 0 < p \leq 1$$

$$(c) f(x) = |x|_p^{\beta}, \beta \geq 1$$

$$1 + 2^{-1} + 2^{-2} + \dots + 2^{-n} + \dots = 2$$

$$S_n = 1 + 2^{-1} + \dots + 2^{-n} = \frac{2^{n+1} - 1}{2^{n+1}} = 2 - 2^{-n}$$

$2 - 2^{-n}$  is getting "close" to 2 in the sense measured by conditional absolute value

given  $\epsilon > 0$ ,  $|2 - (2 - 2^{-n})| < \epsilon$  if  $n \gg 0$

We'll replace the usual absolute value  $|\cdot|$  with the  $p$ -adic absolute value  $|\cdot|_p$

$$x, y \in \mathbb{Z}_p$$

" $x+y$  close"  
 $p$ -adically

$$|x-y|_p \text{ small}$$

this should be a small real number

$$|x-y|_p \leq p^{-m}$$



$$\text{ord}_p(x-y) \geq m \iff x-y \in p^m \mathbb{Z}_p \text{ (i.e. } p^m | x-y)$$

$$-1 + 1 + 2 + 2^2 + \dots$$

$$2\text{-adic expansion } S_n = -1 + 1 + 2 + \dots + 2^n \equiv \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$$

$$|-2 - S_n|_2 = (-1 - (-1 + 2^{n+1}))|_2 = |2^{n+1}|_2 = 2^{-1-n}$$

small if  
n large

Sequences series ( $p$ -adically)

e.g.  $a_n \in \mathbb{Q}_p$  sequence,  $N \geq 0$

converges to  $a$  means

for  $\epsilon > 0$  s.t.  $|a - a_n|_p < \epsilon$  if  $n > N_\epsilon$ :  $\exists N_\epsilon \geq 0$

natural candidates for convergent sequences:

Cauchy sequences:  $\{a_n\}$  s.t. for  $\epsilon > 0$  s.t.  $\{a_n - a_m\} \in \mathbb{Q}$

In  $\mathbb{Q}_p$  every Cauchy sequence

$$\exists N_\epsilon \geq 0$$

$$N_{n,m} > N_\epsilon$$

converges.  $a_n = p^{k_n} u_n$   $k_n \in \mathbb{Z}$

$$u_n \in \mathbb{Z}_p^\times$$

$k_n$  unbounded:  $2^{k_n} \rightarrow \infty$   $p$ -adically

$k_n$  bounded:  $f_n \in \mathbb{Q}$   $|p^{k_n} u_n - p^{k_m} u_m|_p < p^{-j}$   $j \gg 0$

$$-1, 0, 1, \dots, -k_m k_m, 1$$

$$|\rho^{k} u_n - \rho^k v_n|_p < p^{-j} \quad j \gg 0$$

$|u_n - v_n|_p < p^{-j}$

$$u_n \equiv v_n \pmod{p^k} \quad \forall n, m \gg 0$$

Every element of  $\mathbb{Q}_p$  is the limit of a Cauchy sequence of rational numbers.

$x \in \mathbb{Q}_p, \exists \{\gamma_n\}$  c.s. s.t.  $\{\gamma_n\} \rightarrow x; \gamma_n \in \mathbb{Q}$

$$x = p^k a; a = \sum_{n=0}^{\infty} a_n; a_n \in \mathbb{Z}/p^n; a_{n+1} \equiv a_n \pmod{p^n}$$

[can assume]  $a_n \equiv \gamma_n \pmod{p^n}; \gamma_n \in \mathbb{R}_n$

The  $\{\gamma_n\}$  is a sequence of rational numbers

$$\gamma_n = \sum_{i=0}^{n-1} c_i p^i, c_i \in \mathbb{R}_i = \{0, 1, \dots, p-1\}.$$

$$|\gamma_n - \gamma_m| = \left| \sum_{i=n}^{m-1} c_i p^i \right|_p = |p^m|_p \cdot |c_n c_{n+1} p + \dots + c_{m-1} p^{m-n-1}|_p \leq p^{-n}$$

$$u = \sum_{n=0}^{\infty} a_n \pmod{p^m}; u - \gamma_n = \underbrace{\sum_{m=n}^{\infty} \gamma_n - \gamma_m \pmod{p^m}}$$

$$p^m \mid u - \gamma_n \quad \text{" if } m \geq n$$

$$|u - \gamma_n| \leq p^{-m} \text{ so } \{\gamma_n\} \rightarrow u$$

$$\sum_{i=0}^{\infty} c_i p^i = 0 \text{ in } \mathbb{Q}_p$$

$\mathcal{C}_p$  = set of ( $p$ -adic) Cauchy sequences

$$\{\gamma_n\}, \gamma_n \in \mathbb{Q} \text{ w.r.t. } |\cdot|_p$$

• ring under mult. + addition of sequences.

$\mathcal{C}_p \rightarrow \mathbb{Q}_p$  kernel of (\*) = set of Cauchy sequences that converge to 0

$$\left\{ \{\gamma_n\} \text{ c.s. s.t. } |\gamma_n|_p \rightarrow 0 \right\} = N_p$$

The:  $\mathcal{C}_p / N_p \xrightarrow{\sim} \mathbb{Q}_p$